Extended security arguments for signature schemes

Özgür Dagdelen, David Galindo, Pascal Véron, Sidi Mohamed El Yousfi Alaoui, Pierre-Louis Cayrel

Noname manuscript No.
(will be inserted by the editor)

Extended Security Arguments for Signature Schemes

Özgür Dagdelen · David Galindo · Pascal Véron · Sidi Mohamed El Yousfi Alaoui · Pierre-Louis Cayrel

Received: date / Accepted: date

Abstract It is known how to transform certain canonical three-pass identification schemes into signature schemes via the Fiat-Shamir transform. Pointcheval and Stern showed that those schemes are existentially unforgeable in the random-oracle model leveraging the, at that time, novel forking lemma. Recently, a number of 5-pass identification protocols have been proposed. Extending the above technique to capture 5-pass identification schemes would allow to obtain novel unforgeable signature schemes. In this paper, we provide an extension of the forking lemma (and the Fiat-Shamir transform) in order to assess the security of what we call n-generic signature schemes. These include signature schemes that are derived from certain $(2n+1)$-pass identification schemes. In doing so, we put forward a generic methodology for proving the security of a number of signature schemes derived from $(2n+1)$-pass identification schemes for $n \geq 2$. As an application of this methodology, we obtain two new code-based existentially-unforgeable signature schemes, along with a security reduction. In particular, we solve an open problem in multivariate cryptography posed by Sakumoto, Shirai and Hiwatari at CRYPTO 2011.

Ö. Dagdelen · S. M. El Yousfi Alaoui
Darmstadt University of Technology, Germany
{oezguer.dagdelen,elyousfi}@cased.de

D. Galindo
LORIA/CNRS, Nancy, France
david.galindo-chacon@loria.fr

SCYTL Secure Electronic Voting, Barcelona, Spain
david.galindo@scytl.com

P. Véron
IML/IMATH Université du Sud Toulon-Var, France
veron@univ-tln.fr

P.-L. Cayrel
Laboratoire Hubert Curien Université de Saint-Etienne, France
pierre.louis.cayrel@univ-st-etienne.fr

Keywords code-based cryptography · multivariate cryptography · signature schemes · forking lemma · identification schemes · Fiat-Shamir

1 Introduction

The focus of this work is on methodologies to prove the security of digital signature schemes. Thus, instead of providing security reductions from scratch, the goal is to provide security arguments for a class of signature schemes, as previously done in [21, 22, 18, 1, 28]. In particular, we aim at extending a pioneering work by Pointcheval and Stern [21] where a reduction technique was introduced to obtain security arguments for the so-called generic signature schemes. These security arguments allow for simple proofs and for efficient signature schemes. Moreover, this type of signature schemes can be derived from identification schemes if the latter satisfy certain requirements.

Generic Signature Schemes. Pointcheval and Stern call generic signature schemes those whose signatures are of the form $\sigma = (\sigma_0, h_1, \sigma_1)$, where σ_0 is uniformly distributed over a large set, $h_1 = H(m, \sigma_0)$ with H being a hash function modeled as a random oracle, m being the message to be signed and σ_1 depends merely on σ_0 and h_1 (and, obviously, on the secret key of the signature scheme).

The works [21, 22] provide security arguments for generic signature schemes thanks to the use of the forking lemma. This lemma states that a successful forger can be reinvoked with a different random oracle in order to get two distinct but related forgeries. If the generic signature schemes additionally enjoy the existence of a polynomial-time algorithm, called *extractor*, that recovers the signing key from two signatures $\sigma = (\sigma_0, h_1, \sigma_1)$ and $\sigma' = (\sigma_0, h'_1, \sigma'_1)$ on the same message with $h_1 \neq h'_1$, then unforgeability is guaranteed under a certain computational assumption. For instance, signature schemes obtained from Σ-protocols fall into this category, thanks to the *special soundness* property of the latter [9].

Unfortunately, the above framework has only addressed 3-tupled generic signatures (3-pass identification schemes). An extension of the forking lemma for signatures of the form $(\sigma_0, h_1, \sigma_1, \ldots, h_n, \sigma_n)$, where $h_i = H_i(m, \sigma_0, h_1, \sigma_1, \ldots, h_{i-1}, \sigma_{i-1})$ for $n \in \mathbb{N}$, would allow to address a greater class of signatures. Roughly speaking, n-generic signature schemes are built as generic signature schemes but are not restricted in the number of tuple entries as mentioned above.

From Identification Schemes to Signature Schemes. One way to build a signature scheme (in the random-oracle model) is to depart from an existing identification protocol and convert it into a signature scheme using the well-known Fiat-Shamir (FS) paradigm [12].[1] In an identification protocol a series of messages are exchanged between two parties, called prover and verifier, in order to enable a prover to convince a verifier that it knows a given secret. Zero-knowledge identification protocols [16] convince a verifier without revealing any other information whatsoever about the secret itself. Informally, the FS paradigm builds a signature scheme as the transcript of one execution of the identification scheme, where the verifier's

[1] Alternatively, one could use Fischlin's transformation [13] in order to derive signature schemes. A comparison between Fiat-Shamir and Fischlin's transformation can be found in [11]

challenges are replaced by the outputs of a secure hash function on input the message and the current transcript.

In [21] the signatures obtained by applying the FS transform to canonical identification schemes were called *generic signatures schemes*. Schematically, in a canonical identification scheme a prover starts the interaction by sending a commitment Com, then it receives a challenge Ch drawn from a uniform distribution by the verifier, and it finishes the interaction with a message, called response Rsp. Finally, the verifier runs a verifying algorithm determining acceptance or rejection. In addition, the identification protocol needs to satisfy *special soundness*. Roughly speaking, special soundness means that there exists a polynomial-time algorithm which is able to extract the witness of the prover, given two correlated transcripts $(\mathsf{Com}, \mathsf{Ch}, \mathsf{Rsp}), (\mathsf{Com}, \mathsf{Ch}', \mathsf{Rsp}')$ with $\mathsf{Ch} \neq \mathsf{Ch}'$.

Many zero-knowledge identification schemes have been proposed whose conversion to signature schemes lead to generic signature schemes [12,14,26]. However, 5-pass identification protocols are not covered by the abstraction above. Thus, we do not know whether a generalization of the Fiat-Shamir transform to 5-pass identification schemes would give raise to unforgeable signature schemes. We are then obliged to prove the security of those signatures schemes from scratch. Examples of schemes falling outside the Pointcheval-Stern framework can be found in [7, 25,26,8,19,20,24,17,27]. The authors must provide direct proofs for the signature schemes in these works deriving from their 5-pass identification protocols. These proofs are often quite complex. Moreover, the authors of [23] left open the problem of finding a security reduction for the signature scheme derived from their newly introduced 5-pass identification protocol.

Our Contributions. Firstly, we provide an extension of the forking lemma for signatures of the form $(\sigma_0, h_1, \sigma_1, \ldots, h_n, \sigma_n)$, where $h_i = H_i(m, \sigma_0, h_1, \sigma_1, \ldots, h_{i-1}, \sigma_{i-1})$ for $n \in \mathbb{N}$, that we call *n-generic signatures*. This definition potentially allows us to capture signature schemes obtained by applying the Fiat-Shamir transformation to n-pass identification schemes. Roughly speaking, n-generic signature schemes are built as generic signature schemes but are not restricted in the number of entries. Our extension of the forking lemma (Theorem 1, Section 3) states that from an adversary $\mathcal{A}$ that with non-negligible probability finds a forgery $\sigma = (\sigma_0, h_1, \sigma_1, \ldots, h_n, \sigma_n)$ on message m it can be obtained (by rewinding) another adversary $\mathcal{A}'$ that obtains a forgery $\sigma' = (\sigma_0, h_1, \sigma_1, \ldots, h'_n, \sigma'_n)$ on m with $h_n \neq h'_n$. We give evidence that 5-pass identification schemes give raise to 2-generic signature schemes

Secondly, we continue by identifying a property, which we call 2-*soundness*, that can be used to prove the unforgeability of 2-generic signatures schemes satisfying it. This property is satisfied by the signature schemes obtained by applying the extended Fiat-Shamir Transform to the 5-pass identification schemes [8,23]. Informally, 2-soundness means that the signing key sk can be extracted from 4 correlated valid signatures on the same message m of the form $\sigma^{(1)} = (\sigma_0, h_1, \sigma_1, h_2^{(1)}, \sigma_2^{(1)})$, $\sigma^{(2)} = (\sigma_0, h'_1, \sigma'_1, h_2^{(2)}, \sigma_2^{(2)})$ with $h_1 \neq h'_1, \sigma_1 \neq \sigma'_1$, and $\sigma^{(3)} = (\sigma_0, h_1, \sigma_1, h_2^{(3)}, \sigma_2^{(3)})$, $\sigma^{(4)} = (\sigma_0, h'_1, \sigma'_1, h_2^{(4)}, \sigma_2^{(4)})$ with $h_2^{(2)} \neq h_2^{(4)}, \sigma_2^{(2)} \neq \sigma_2^{(4)}$ and $h_2^{(1)} \neq h_2^{(3)}, \sigma_2^{(1)} \neq \sigma_2^{(3)}$.

Thirdly, we are able to generalize 2-soundness to n-soundness. Roughly speaking, n-soundness requires that a valid signing key sk can be extracted from 2^n

distinct but correlated signatures on the same message m. Through our Nested Forking Lemma (Theorem 2, Section 4) we are able to leverage our Extended Forking Lemma to show that any forger against an n-generic signature scheme can be recursively run 2^n times to obtain 2^n signatures as required by n-soundness, for n logarithmically upper-bounded in the security parameter.

Fourthly and lastly, we give two concrete instantiations in our framework. With our first instantiation, we solve an open problem in multivariate cryptography, by showing in Section 5 that our methodology encompasses the signature scheme suggested by Sakumoto, Shirai and Hiwatari [23] at CRYPTO 2011. Such a security statement was missing in [23] and was left as an open problem by the authors. We provide an additional second existentially unforgeable signature scheme, by applying our framework to the 5-pass code based identification scheme proposed by Cayrel, El Yousfi Alaoui and Véron in [8].

Related Work. Pointcheval and Stern [21, 22] provide security arguments for generic signature schemes. The latter are restrictive in the sense that (a) they allow transformations only based on canonical identification schemes, and (b) the existence of an extractor is required. The work of Abdalla *et al.* [1] introduced a new transformation from identification schemes (IS) to signature schemes (SS) without insisting on the existence of such an extractor. Nonetheless, they require again canonical IS. Ohta and Okamoto [18] assume that the IS is honest-verifier (perfect) zero-knowledge and that it is computationally infeasible for a cheating prover to convince the verifier to accept. Again, this result is valid only for three-pass IS.

Security arguments for the FS transformation in the standard model can be found in [15, 5]. Moreover, the security of the FS transform against quantum adversaries in the quantum random oracle model [6] is investigated in [10]. In [4], Bellare and Neven stated the forking lemma in a generalized way merely looking at the output behavior of an algorithm if it is run twice on related inputs. They decouple the notion of forking lemma from signature schemes.

Previous Conference Version. This work is based on the contents of a previous conference publication by the authors [3]. We point out that the security arguments sketched in our previous work for the signature scheme by Sakumoto, Shirai and Hiwatari were flawed. Indeed, we claimed that 2 forgeries on the same message m were enough to recover the underlying secret key, while the proof of knowledge argument given in [23] requires in fact 4 such forgeries. To fix our previous security argument we have introduced the Nested Forking Lemma in Section 4, which indeed works for any n-signature for $n \geq 1$.

Organization. We introduce in Section 2 the technical machinery needed to state and prove our results. In Section 3 we present the notion of n-generic signature schemes and provide an extended forking lemma that applies to this new signature class. We state and prove in Section 4 the Nested Forking Lemma. In Sections 5 we apply our paradigm and derive two new provably secure 2-generic signature schemes; one based on multivariate polynomials and another one based on q-ary codes.

2 Preliminaries

We begin by introducing some notations and briefly reviewing some definitions. A function $\mu(\cdot)$ is *negligible in* n, or just *negligible*, if for every positive polynomial $p(\cdot)$ and all sufficiently large n it holds that $\mu(n) < 1/p(n)$. Otherwise, we call $\mu(\cdot)$ *non-negligible*. Note that the sum of two negligible functions (resp. non-negligible) is again negligible (resp. non-negligible) whereas the sum of one non-negligible function $\pi(\cdot)$ and one negligible function $\mu(\cdot)$ is non-negligible, i.e. there exists a positive polynomial $p(\cdot)$ such that for infinitely many n's it holds that $\pi(n)+\mu(n) > 1/p(n)$.

Two distributions ensembles $\{X_n\}_{n\in\mathbb{N}}$ and $\{Y_n\}_{n\in\mathbb{N}}$ are said to be *(computationally) indistinguishable*, if for every non-uniform polynomial-time algorithm D, there exists a negligible function $\mu(\cdot)$ such that

$$|\Pr[\,D(X_n) = 1] - \Pr[\,D(Y_n) = 1]| \leq \mu(n)\ .$$

A random variable X has min-entropy k, denoted $H_\infty(X) = k$, if

$$\max_x \Pr[X = x] = 2^{-k}.$$

We write $s \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}(x)$ to denote the output s by a probabilistic algorithm $\mathcal{A}$ with input x having black-box access to an oracle $\mathcal{O}$. In particular, this means, that $\mathcal{A}$ may query oracle $\mathcal{O}$ in order to derive s from its answers. An algorithm $\mathcal{A}$ is probabilistic polynomial-time (PPT) if $\mathcal{A}$ is randomized and for any input $x \in \{0,1\}^*$ the computation of $\mathcal{A}(x)$ terminates in at most $poly(|x|)$ steps.

Digital Signatures. In the following we give the definition of a signature scheme together with the corresponding standard security level.

Definition 1 (Signature scheme) A signature scheme is a collection of the following algorithms $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ defined as follows.

$\mathsf{KGen}(1^\kappa)$ is a probabilistic algorithm which, on input a security parameter 1^κ, outputs a secret and a public key $(\mathsf{sk}, \mathsf{pk})$.

$\mathsf{Sign}(\mathsf{sk}, m)$ is a probabilistic algorithm which, on input a secret key sk and a message m, outputs a signature σ.

$\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ is a deterministic algorithm which, on input a public key pk, a message m and a signature σ, outputs either 1 (= valid) or 0 (= invalid).

We require correctness of the verification, i.e., the verifier will always accept genuine signatures. More formally, for all $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\kappa)$, any message m, any $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$, we always have $\mathsf{Vf}(\mathsf{pk}, m, \sigma) = 1$. This requirement can be relaxed to hold only with overwhelming probability.

Additionally we assume the existence of an algorithm $\mathsf{Test}(\mathsf{pk}, \mathsf{sk})$ such that it outputs 1 iff $(\mathsf{sk}, \mathsf{pk})$ belongs to the output space $\mathsf{KGen}(1^\kappa)$. This requirement can be relaxed to hold only with overwhelming probability.

From signature schemes we require that no outsider should be able to forge a signer's signature. The following definition captures this property formally.

Definition 2 (Unforgeability of a Signature Scheme) A signature scheme $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ is existentially unforgeable under (adaptively) chosen-message attacks if for any PPT algorithm $\mathcal{A}$ making at most q_s queries to oracle OSign, the probability that the following experiment returns 1 is negligible:

Experiment $\mathsf{Unforgeability}^{\mathrm{S}}_{\mathcal{A}}(\kappa)$
$(\mathsf{sk}, \mathsf{pk}) \xleftarrow{\$} \mathsf{KGen}(1^{\kappa})$
$(\sigma^*, m^*) \xleftarrow{\$} \mathcal{A}^{\mathsf{OSign}}(\mathsf{pk})$
$\mathsf{OSign}(\cdot)$ on input m outputs $\sigma \xleftarrow{\$} \mathsf{Sign}(\mathsf{sk}, m)$
Return 1 iff
$\mathsf{Vf}(\mathsf{pk}, m^*, \sigma^*) = 1$ and m^* was not queried to $\mathsf{OSign}(\cdot)$ by $\mathcal{A}$

The probability is taken over all coin tosses of KGen, Sign, and $\mathcal{A}$.

Note that q_s is bounded by a polynomial in the security parameter κ. Definition 2 captures unforgeability against adaptively chosen-message attacks for signature schemes. Unforgeability against no-message attacks is obtained from the above by setting $q_s = 0$.

Splitting Lemma. The following lemma is extensively used in the forking lemma proofs. It states that one can split a given set X into two subsets, (a) a non-negligible subset Ω consisting of "good" x's which provides a non-negligible probability of success over y, and (b) its complement, consisting of "bad" x's.

Lemma 1 (Splitting Lemma [21, Lemma 3]) *Let A be a subset of $X \times Y$ such that $Pr[A(x, y)] \geq \epsilon$, then there exist $\Omega \subset X$ such that*

1. *$Pr[x \in \Omega] \geq \epsilon/2$*
2. *If $a \in \Omega$, then $Pr[A(a, y)] \geq \epsilon/2$.*

3 Extended Forking Lemma

In this section we give the formal definition of an n-generic signature scheme and extend the forking lemma accordingly.

3.1 n-Generic Signature Schemes

Let H_i denote a hash function with output of cardinality 2^{κ_i} (where each κ_i can be written as a polynomial in the security parameter κ).

Definition 3 (n-Generic Signature Scheme) Let $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ be a signature scheme with an additional algorithm Test such that $\Pr[\mathsf{Test}(\mathsf{pk}, \mathsf{sk}) = 1 : \exists r \text{ s.t. } (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(\kappa; r)] = 1$ (except for negligible probability). We say that S is a n-generic signature scheme if the following properties are satisfied:

Structure. A signature σ for a message m is of the form $(\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ where $h_1 = H_1(m, \sigma_0)$ and $h_i = H_i(m, \sigma_0, \ldots, h_{i-1}, \sigma_{i-1})$ for $i = 2, \ldots, n$ with H_i being modeled as a random oracle. Each σ_i can depend on previous signature blocks $\sigma_0, \ldots, \sigma_{i-1}$ and hash values $h_1, \ldots, h_i$ for $i = 1, \ldots, n$ (and, obviously, also from public and secret key of the signer). We require that the min-entropy of the random variable which outputs $\sigma_0, \ldots, \sigma_{n-1}$ must be in $\omega(|H_n|)$.[2]

[2] This requirement is necessary for Lemma 3.

Honest-Verifier Zero-Knowledge (HVZK). Assume the hash functions H_i are instantiated via publicly accessible random oracles. There exists a PPT algorithm Z, the *zero-knowledge simulator*, controlling the random oracles, such that for any pair of PPT algorithms $D = (D_0, D_1)$ the following distributions are computationally indistinguishable:
- Let $(\mathsf{pk}, \mathsf{sk}, m, state) \leftarrow D_0(1^\kappa)$. If $\mathsf{Test}(\mathsf{pk}, \mathsf{sk}) = 1$, then set $\sigma := (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n) \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$; else $\sigma \leftarrow \perp$. Output $D_1(\sigma, state)$.
- Let $(\mathsf{pk}, \mathsf{sk}, m, state) \leftarrow D_0(1^\kappa)$. If $\mathsf{Test}(\mathsf{pk}, \mathsf{sk}) = 1$, then set $\sigma := (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n) \leftarrow Z(\mathsf{pk}, m, 1)$; else $\sigma \leftarrow Z(\mathsf{pk}, m, 0)$. Output $D_1(\sigma, state)$.

Notice that the structure of a generic signature as originally proposed in [21] matches that of a 1-generic signature following our definition. We occasionally write $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_n, h_1 \ldots, h_n)$ instead of $(\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ for the sake of readability.

In the following we show that, perhaps surprisingly, every n-generic signature scheme can actually be seen as a $(n-1)$-generic signature scheme. We will heavily use this fact in the proof of the Nested Forking Lemma (Theorem 2, Section 4).

Lemma 2 (n-generic signature $\Rightarrow$ $(n-1)$-generic signature) *Let* S *be a n-generic signature scheme outputting signatures of the form $\sigma = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$. Let $\mathrm{S}^\dagger$ be the signature scheme obtained from* S *by setting the output signatures $\sigma^\dagger$ to be $\sigma^\dagger = (\sigma_0, h_1, \ldots, h_{n-1}, \sigma^\dagger_{n-1})$, where $\sigma^\dagger_{n-1} := (\sigma_{n-1}, h_n, \sigma_n)$. Then $\mathrm{S}^\dagger$ is a $(n-1)$-generic signature scheme.*

Proof It is easy to see that:

- $\mathrm{S}^\dagger$ has the structure of a $(n-1)$-generic signature scheme if S has the structure of a n-generic signature scheme;
- $\mathrm{S}^\dagger$ has the honest-verifier zero-knowledge if σ does. Indeed, define $Z^\dagger(\mathsf{pk}, m, 1) := (\sigma_0, h_1, \ldots, \sigma^\dagger_{n-1})$, where $\sigma := (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n) \leftarrow Z(\mathsf{pk}, m, 1)$. □

3.2 An Extended Forking Lemma – No-Message Attack Model

Pointcheval and Stern introduced in [21] the forking lemma as a technique to prove the security of some families of signature schemes, namely generic signature schemes with special soundness. This well-known lemma is applied to get two forgeries for the same message using a replay attack. After that, one can use those two forgeries to recover the secret key. They also show that a successful forger in the adaptive chosen-message attack model implies a successful forger in the no-message attack model, as long as the honest-verifier zero-knowledge property holds. In the following we propose an extension of the original forking lemma that can be applied to n-generic signature schemes. We first provide the Extended Forking Lemma in the no-message attack model.

Lemma 3 *Let* S *be an n-generic signature scheme with security parameter κ. Let $\mathcal{A}$ be a PPT algorithm given only the public data as input. Assume that $\mathcal{A}$, after querying the n random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$ polynomially often in κ, outputs a valid signature $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ for message m with a non-negligible probability. Let us consider a replay of this machine $\mathcal{A}$ with the same random tape (as a Turing*

machine), the same responses to the queries corresponding to $\mathcal{O}_1, \ldots, \mathcal{O}_{n-1}$, but a different output to exactly one query to $\mathcal{O}_n$. Then running $\mathcal{A}$ and its reply results in two valid signatures $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ and $(\sigma_0, \ldots, \sigma'_n, h_1, \ldots, h'_n)$ for the same message m and $h_n \neq h'_n$ with a non-negligible probability.

Proof We are given a no-message adversary $\mathcal{A}$, which is a PPT Turing machine with a random tape ω taken from a set R_ω. During the attack, $\mathcal{A}$ may ask $q_1, \ldots, q_n$ queries to random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$, respectively. We denote by $q_1^{(i)}, \ldots, q_{q_i}^{(i)}$ the q_i distinct queries to the random oracle $\mathcal{O}_i$ and let $r^{(i)} = (r_1^{(i)}, \ldots, r_{q_i}^{(i)})$ be the corresponding answers, where $r_j^{(i)}$ is the answer to the j-th query to $\mathcal{O}_i$, for $1 \leq i \leq n$ and $1 \leq j \leq q_i$. Let $S_i^{q_i}$ denote the set of all possible answers from $\mathcal{O}_i$, thus $(r_1^{(i)}, \ldots, r_{q_i}^{(i)}) \subset S_i^{q_i}$. Furthermore, we denote by

$\mathcal{E}$: the event that $\mathcal{A}$ can produce a valid signature $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ for message m by using random tape ω and the answers $r_1^{(i)}, \ldots, r_{q_i}^{(i)}$ for $1 \leq i \leq n$. Note that a valid signature implies $h_i = \mathcal{O}_i(m, \sigma_0, h_1, \ldots, h_{i-1}, \sigma_{i-1})$.

$\mathcal{F}$: the event that $\mathcal{A}$ queried the oracle $\mathcal{O}_n$ on input $(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})$, i.e.,

$$\exists l \in \{1, \ldots, q_n\} : \; q_l^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \; .$$

Accordingly, its complement $\neg\mathcal{F}$ denotes

$$\forall l \in \{1, \ldots, q_n\} : \; q_l^{(n)} \neq (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \; .$$

By hypothesis of the lemma, the probability that event $\mathcal{E}$ occurs is non-negligible, namely there exists a polynomial function $T(\cdot)$ such that $\Pr[\mathcal{E}] \geq \frac{1}{T(\kappa)}$. We know that

$$\Pr[\mathcal{E}] = \Pr[\mathcal{E} \wedge \; \mathcal{F}] + \Pr[\mathcal{E} \wedge \; \neg\mathcal{F}] \tag{1}$$

Furthermore, we get

$$\begin{aligned}
&\Pr[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \wedge \neg\mathcal{F}] \\
&\quad = \Pr[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \mid \neg\mathcal{F}] \cdot \Pr[\neg\mathcal{F}] \\
&\quad \leq \Pr[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \mid \neg\mathcal{F}] \\
&\quad \leq \frac{1}{2^{\kappa_n}},
\end{aligned}$$

because the output of $\mathcal{O}_n$ is unpredictable and $(m, \sigma_0, \ldots, \sigma_{n-1})$ has a sufficient min-entropy given the definition of n-generic signature. Event $\mathcal{E}$ implies that $h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})$, and thus we get

$$\Pr[\mathcal{E} \wedge \neg\mathcal{F}] \leq \Pr[h_n = \mathcal{O}_n(m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}) \wedge \neg\mathcal{F}] \leq \frac{1}{2^{\kappa_n}} \tag{2}$$

Inequalities (1) and (2) lead to

$$\Pr[\mathcal{E} \wedge \; \mathcal{F}] \geq \frac{1}{T(\kappa)} - \frac{1}{2^{\kappa_n}} \geq \frac{1}{T'(\kappa)} \tag{3}$$

Note that a polynomial $T'(\cdot)$ must exist since the difference between a non-negligible and negligible term is non-negligible. Therefore, $\exists l \in \{1, \ldots, q_n\}$ so that

$$\Pr\left[\mathcal{E} \wedge q_l^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\right] \geq \frac{1}{q_n T'(\kappa)}.$$

Indeed, if we suppose that, $\forall l \in \{1, \ldots, q_n\}$,

$$\Pr\Big[\mathcal{E} \wedge q_l^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\Big] < \frac{1}{q_n T'(\kappa)}$$

then,

$$\begin{aligned}\Pr[\mathcal{E} \wedge \ \mathcal{F}] &= \Pr\Big[\mathcal{E} \wedge (\exists j \leq q_n, q_j^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1}))\Big] \\ &\leq \sum_{j=1}^{q_n} \Pr\Big[\mathcal{E} \wedge q_j^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\Big] \\ &< \frac{q_n}{q_n T'(\kappa)} = \frac{1}{T'(\kappa)}\end{aligned}$$

This leads to a contradiction with (3). Further, we define

$$B = \{(\omega, r^{(1)}, \ldots, r^{(n)}) \text{ s.t. } \mathcal{E} \wedge q_l^{(n)} = (m, \sigma_0, h_1, \ldots, h_{n-1}, \sigma_{n-1})\}.$$

Since, $B \subset R_\omega \times S_1^{q_1} \times \ldots \times S_n^{q_n}$ and $\Pr[B] \geq \frac{1}{q_n T'(\kappa)}$, by using the splitting lemma we have:

- $\exists \Omega \subset R_\omega$ such that $\Pr[\omega \in \Omega] \geq \frac{1}{2q_n T'(\kappa)}$.
- $\forall \omega \in \Omega$, $\Pr\Big[(\omega, r^{(1)}, \ldots, r^{(n)}) \in B\Big] \geq \frac{1}{2q_n T'(\kappa)}$, where the probability is taken over $S_1^{q_1} \times \ldots \times S_n^{q_n}$.

We define

$$B' = \{(\omega, r^{(1)}, \ldots, r^{(n)}) \text{ s.t. } (\omega, r^{(1)}, \ldots, r^{(n)}) \in B \wedge \omega \in \Omega\}.$$

Recall that $r^{(i)} = (r_1^{(i)}, \ldots, r_{q_i}^{(i)})$ where $r_j^{(i)} \in S_i$ for $1 \leq j \leq q_i$. Since,

$$B' \subset (R_\omega \times S_1^{q_1} \times \ldots \times S_n^{l-1}) \times S_n^{q_n - l + 1},$$

by using the splitting lemma again we get

- $\exists \Omega' \subset R_\omega \times S_1^{q_1} \times \ldots \times S_n^{l-1}$ such that $\Pr\Big[(\omega, r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)})) \in \Omega'\Big] \geq \frac{1}{4q_n T'(\kappa)}$.
- $\forall (\omega, r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)})) \in \Omega'$, $\Pr\Big[(\omega, r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)}, r_l^{(n)}, \ldots, r_{q_n}^{(n)})) \in B'\Big] \geq \frac{1}{4q_n T'(\kappa)}$, where the probability is taken over $S_n^{q_n - l + 1}$.

As a result, if we choose l, ω, $(r^{(1)}, \ldots, r^{(n-1)}, (r_1^{(n)}, \ldots, r_{l-1}^{(n)}), (r_l^{(n)}, \ldots, r_{q_n}^{(n)})$, and $(r'^{(n)}_l, \ldots, r'^{(n)}_{q_n})$ randomly, then we obtain two valid signatures $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ and $(\sigma_0, \ldots, \sigma'_n, h_1, \ldots, h'_n)$ for message m such that $h_n \neq h'_n$ with a non-negligible probability.[3]

□

[3] Since l is the index of $\mathcal{A}$'s query and there are only polynomially number of queries made by $\mathcal{A}$, our success probability remains non-negligible when picking l randomly.

3.3 Extended Forking Lemma – Chosen-Message Attack Model

We now provide the Extended Forking Lemma in the adaptively chosen-message attack model. In this model, an adversary may adaptively invoke a signing oracle and is successful if it manages to compute a signature on a new message. If the signing oracle outputs signatures which are indistinguishable from a genuine signer without knowing the signing key, then using the simulator one can obtain two distinct signatures with a suitable relation from a single signature, similarly to the no-message scenario.

Theorem 1 (The Chosen-Message Extended Forking Lemma) *Let* S *be an n-generic signature scheme with security parameter κ. Let $\mathcal{A}$ be a PPT algorithm given only the public data as input. Let us assume that $\mathcal{A}$, after querying the n random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$ and the signer polynomially often in κ, can find a valid signature $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ for message m with a non-negligible probability. Then, there exists another PPT algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine, that replaces interactions between $\mathcal{A}$ and its challenger by a simulation, and which provides with a non-negligible probability two valid signatures $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ and $(\sigma_0, \ldots, \sigma'_n, h_1, \ldots, h'_n)$ for the same message m such that $h_n \neq h'_n$.*

Proof We consider a PPT algorithm $\mathcal{B}$ that executes $\mathcal{A}$ in such a way that $\mathcal{B}$ simulates the environment of $\mathcal{A}$. Therefore, $\mathcal{B}$ must simulate the interactions of $\mathcal{A}$ with random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$ and with the real signer. Then, we could see $\mathcal{B}$ as an algorithm performing a no-message attack against the signature scheme S.

Let Sim denote the zero-knowledge simulator of S that can simulate the answers of the real signer without knowledge of the secret key and has access to $\mathcal{O}_i$ $(1 \leq i \leq n)$. Let $\mathcal{A}$ be an adaptively chosen-message adversary, which is a probabilistic polynomial time Turing machine with a random tape ω taken from a set R_ω. During the attack, $\mathcal{A}$ may ask $q_1, \ldots, q_n$ queries to random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$, and q_s queries (possibly repeated) to Sim. The values $q_1, \ldots, q_n$ and q_s are polynomially bounded in κ. We denote by $q_1^{(i)}, \ldots, q_{q_i}^{(i)}$ the q_i distinct queries to the random oracles $\mathcal{O}_i$, and by $m^{(1)}, \ldots, m^{(q_s)}$ the q_s queries to the simulator Sim.

The simulator Sim answers a tuple $(\sigma_0^{(j)}, \ldots, \sigma_n^{(j)}, h_1^{(j)}, \ldots, h_n^{(j)})$ as a signature for a message $m^{(j)}$, for each integer j with $1 \leq j \leq q_s$. Then, the adversary $\mathcal{A}$ assumes that $h_i^{(j)} = \mathcal{O}_i(m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)})$ holds for all $1 \leq i \leq n$ and $1 \leq j \leq q_s$, and stores all these relations.

Now we need to consider potential "collisions" of queries in the random oracles. There are two kind of collisions that can appear. That is, (a) the simulator Sim queries the random oracle with the same input the adversary has asked before (let us denote this event by $\mathcal{E}_1$), and (b) Sim asks the same question repeatedly (let us denote this event by $\mathcal{E}_2$).

We show that the probabilities of such events are negligible.

$$\Pr[\mathcal{E}_1] = \Pr[\exists i \in \{1, \ldots, n\}; \exists j \in \{1, \ldots, q_s\}; \exists t \in \{1, \ldots, q_n\} | (m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = q_t^{(i)}]$$

$$\leq \sum_{i=1}^{n} \sum_{j=1}^{q_s} \sum_{t=1}^{q_n} \Pr[(m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = q_t^{(i)}] \leq \frac{n q_s q_n}{2^\kappa},$$

which is negligible, assuming that the σ_i's are random values drawn from a large set with cardinality greater than 2^κ.
Moreover, we have

$$\Pr[\mathcal{E}_2] = \Pr[\exists i \in \{1,\ldots,n\}; \exists j, j' \in \{1,\ldots,q_s\} : j \neq j' \mid (m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = (m^{(j')}, \sigma_0^{(j')}, h_1^{(j')}, \ldots, h_{i-1}^{(j')}, \sigma_{i-1}^{(j')})]$$

$$\leq \sum_{i=1}^{n} \sum_{j=1}^{q_s} \sum_{j' \neq j}^{q_s} \Pr[(m^{(j)}, \sigma_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}, \sigma_{i-1}^{(j)}) = (m^{(j')}, \sigma_0^{(j')}, h_1^{(j')}, \ldots, h_{i-1}^{(j')}, \sigma_{i-1}^{(j')})] \leq \frac{nq_s^2}{2^\kappa},$$

which is also negligible.

Algorithm $\mathcal{B}$ succeeds whenever the machine $\mathcal{A}$ produces a valid signature without any collisions. Hence, we have

$$\Pr[\mathcal{B} \text{ succeeds }] = \Pr[\mathcal{A} \text{ succeeds }] - \Pr[\mathcal{E}_1] - \Pr[\mathcal{E}_2] \geq \frac{1}{T(\kappa)} - \frac{nq_sq_n}{2^\kappa} - \frac{nq_s^2}{2^\kappa},$$

which is non-negligible.

Summing up, we have an algorithm $\mathcal{B}$ that performs a no-message attack against the signature scheme S in polynomial time with non-negligible probability of success. Thus, we can use Lemma 3 applied to algorithm $\mathcal{B}$, and we will obtain two valid signatures for the same message, such that $h_n \neq h'_n$ again in polynomial time.

□

4 Nested Forking Lemma

Contrary to the standard forking lemma [21], our extended forking lemma works for n-generic signature schemes. These signatures contain n hash functions which output $h_1, \ldots, h_n$. In Theorem 1 we have shown that given an adversary which outputs a forgery, we can obtain a second correlated one which differs in the last hash output ($h_n \neq h'_n$) (and possibly $\sigma_n \neq \sigma'_n$).

Here, we show that from an n-generic signature scheme and a forgery on message m, one can actually derive 2^n distinct signatures on message m for n logarithmically upper-bounded in the security parameter. To this end, we leverage Lemma 2 and start by viewing the n-generic signature scheme as a 1-generic signature scheme. We derive recursively 2^n forgeries by moving from h_i to h_{i+1}. That is, at each level i for each adversary which outputs eventually a signature on a given message m, we derive two new adversaries outputting two different signatures on m, ending up with 2^n distinct signatures on the same message m.

Theorem 2 (Nested Forking Lemma) *Let* S *be an n-generic signature scheme with security parameter 1^κ. Let $\mathcal{A}$ be a PPT algorithm that is only given public data as input. Let us assume that $\mathcal{A}$, after querying the n random oracles $\mathcal{O}_1, \ldots, \mathcal{O}_n$ and the signer polynomially often in κ, can find a valid signature $(\sigma_0, \ldots, \sigma_n, h_1, \ldots, h_n)$ for message m with a non-negligible probability. Then, there exists another PPT algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as a subroutine, that replaces*

interactions between $\mathcal{A}$ and its challenger by a simulation and which provides, with a non-negligible probability, 2^n valid signatures for the same message m. $\mathcal{B}$ outputs signatures $\sigma^{(i)}$ of the form

$$\sigma^{(i)} = (\sigma_0, \sigma_1^{(i)}, \ldots, \sigma_n^{(i)}, h_1^{(i)}, h_2^{(i)}, \ldots, h_n^{(i)}),$$

where $\sigma_k^{(i)} = \sigma_k^{(i')}$ and $h_k^{(i)} = h_k^{(i')}$ for all i, i' where either $\log(i) > k$ or $\log(i') > k$, and $h_k^{(i)} \neq h_k^{(i')}$ for all i, i' where $\log(i) \leq k$ and $\log(i') \leq k$, for $k = 1, \ldots, n$ and $i \in [1, 2^n]$.

Proof We have shown in Lemma 2 that any n-generic signature scheme is also an $(n-1)$-generic signature scheme. Consequently, by using a recursive argument, any n-generic signature scheme can be interpreted as a 1-generic signature scheme, where signatures are shaped as $(\sigma_0, h_1, \Sigma_1)$, with $\Sigma_1 = (\sigma_1, \ldots, \sigma_n, h_2, \ldots, h_n)$. Let S_1 be the corresponding 1-generic signature scheme. Then any successful adversary $\mathcal{A}$ against the unforgeability of S is also successful against the unforgeability of S_1 with identical success probability, and vice versa, because the signatures and their verification algorithms are essentially identical.

The algorithm $\mathcal{B}$ leverages $\mathcal{A}$ and proceeds exactly as in the Extended Forking Lemma on the signature scheme S_1, but deviates from it in the following way. Instead letting the algorithm in the forking lemma output two signatures, it merely will output the fresh one. Let $\mathcal{A}_2$ be the algorithm (i.e., the forger) which outputs the signature correlated to the signature of $\mathcal{A}$, henceforth denoted by $\mathcal{A}_1$. That is, $\mathcal{B}$ can make use of two forgers $\mathcal{A}_1$ and $\mathcal{A}_2$ which output valid signatures $(\sigma_0, h_1^{(1)}, \Sigma_1^{(1)})$ and $(\sigma_0, h_1^{(2)}, \Sigma_1^{(2)})$, respectively, where $h_1^{(1)} \neq h_1^{(2)}$.

Now, $\mathcal{B}$ repeats the process with both algorithms $\mathcal{A}_1$ and $\mathcal{A}_2$, in order to derive two more forgers $\mathcal{A}_3$ and $\mathcal{A}_4$ which output valid signatures correlated to the ones from $\mathcal{A}_1$ and $\mathcal{A}_2$. Hence, following the notation introduced in the statement of this theorem, the four forgers output the following:

- $\mathcal{A}_1$ outputs $(\sigma_0, \sigma_1^{(1)}, \ldots, \sigma_n^{(1)}, h_1^{(1)}, \ldots, h_n^{(1)})$,
- $\mathcal{A}_2$ outputs $(\sigma_0, \sigma_1^{(2)}, \ldots, \sigma_n^{(2)}, h_1^{(2)}, \ldots, h_n^{(2)})$,
- $\mathcal{A}_3$ outputs $(\sigma_0, \sigma_1^{(3)}, \ldots, \sigma_n^{(3)}, h_1^{(3)}, \ldots, h_n^{(3)})$,
- $\mathcal{A}_4$ outputs $(\sigma_0, \sigma_1^{(4)}, \ldots, \sigma_n^{(4)}, h_1^{(4)}, \ldots, h_n^{(4)})$,

where $(h_1^{(1)}, \sigma_1^{(1)}) = (h_1^{(3)}, \sigma_1^{(3)})$ and $(h_1^{(2)}, \sigma_1^{(2)}) = (h_1^{(4)}, \sigma_1^{(4)})$. We stress that $\mathcal{A}_2$, $\mathcal{A}_3$ and $\mathcal{A}_4$ output a valid signature with non-negligible probability if $\mathcal{A}$ does, a claim that follows from Theorem 1.

The last step is repeated successively and the Extended Forking Lemma is applied to obtain forgeries which differ in the very last hash value h_i. In every round i we obtain 2^{i-1} new forgers (and resp. forgeries), so that we end up with 2^n correlated signatures of the form

$$\sigma^{(i)} = (\sigma_0, \sigma_1^{(i)}, \ldots, \sigma_n^{(i)}, h_1^{(i)}, h_2^{(i)}, \ldots, h_n^{(i)})$$

where $\sigma_k^{(i)} = \sigma_k^{(i')}$ and $h_k^{(i)} = h_k^{(i')}$ for all i, i' where either $\log(i) > k$ or $\log(i') > k$, and $h_k^{(i)} \neq h_k^{(i')}$ for all i, i' where $\log(i) \leq k$ and $\log(i') \leq k$, for $k = 1, \ldots, n$.

Figure 1 illustrates how those signatures are formed and generated. Basically, algorithm $\mathcal{B}$ builds up a tree of correlated signatures starting from the given forger

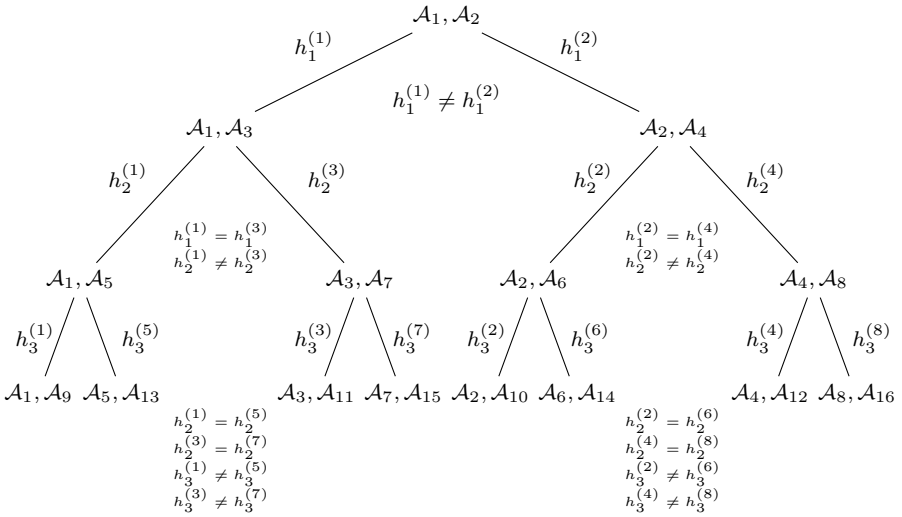

Fig. 1 Forking-Tree with depth 4 for a n-signature scheme. By $\mathcal{A}_i$ we denote the algorithm (i.e., the forger) which outputs signature $\sigma^{(i)} = (\sigma_0, \sigma_1^{(i)}, \ldots, \sigma_n^{(i)}, h_1^{(i)}, h_2^{(i)}, \ldots, h_n^{(i)})$.

$\mathcal{A}$ $(= \mathcal{A}_1)$. Theorem 1 guarantees that $\mathcal{B}$ given a forger will obtain black-box access to an additional forger in polynomial time, where the latter's probability to output a valid signature is non-negligible as long as the former forger has non-negligible advantage. Because $\mathcal{B}$ performs 2^{n-1} times the procedure of Theorem 1, as long as $n = o(\log \kappa)$, $\mathcal{B}$ terminates in polynomial time.

□

5 Applications

In this section we first discuss a transformation from $(2n+1)$-pass identification protocols with a special structure to signature schemes that in many cases yields n-generic signature schemes. This is essentially an extended Fiat-Shamir transform. Then, we go on with two specific instances of the aforementioned transformation. We derive two signature schemes whose security is shown by applying our results from the previous section. These signatures are derived from the five-pass identification scheme based on MQ-problem, recently introduced in [23], and the q-SD code-based five-pass identification scheme [8].

5.1 Security of n-generic Signature Schemes

Our aim is to prove that any n-generic signature scheme satisfying what we call n-soundness is existentially unforgeable in the random-oracle model. To guarantee security under chosen-message attacks, and similarly to generic signature schemes [21], we require a property from n-generic signature schemes that we call n-soundness. Informally, n-soundness means that the secret key can be extracted from 2^n distinct valid signatures $\sigma^{(i)} = (\sigma_0, \sigma_1^{(i)}, \ldots, \sigma_n^{(i)}, h_1^{(i)}, h_2^{(i)}, \ldots, h_n^{(i)})$, where

$\sigma_k^{(i)} = \sigma_k^{(i')}$ and $h_k^{(i)} = h_k^{(i')}$ for all i, i' where either $\log(i) > k$ or $\log(i') > k$), and $h_k^{(i)} \neq h_k^{(i')}$ for all i, i' where $\log(i) \leq k$ and $\log(i') \leq k$, for $k = 1, \ldots, n$ and $i \in [1, 2^n]$. For $n = 1$ it is easy to see that the latter boils down to soundness as originally defined in [21].

Definition 4 (n-Soundness) Let $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ be an n-generic signature scheme. We call S n-sound, if there exists a PPT algorithm K, the knowledge extractor, such that for any κ and m, any $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KGen}(1^\kappa)$, any collection of 2^n distinct valid signatures $\sigma^{(i)} = (\sigma_0, \sigma_1^{(i)}, \ldots, \sigma_n^{(i)}, h_1^{(i)}, h_2^{(i)}, \ldots, h_n^{(i)})$, where $\sigma_k^{(i)} = \sigma_k^{(i')}$ and $h_k^{(i)} = h_k^{(i')}$ for all i, i' where either $\log(i) > k$ or $\log(i') > k$, and $h_k^{(i)} \neq h_k^{(i')}$ for all i, i' where $\log(i) \leq k$ and $\log(i') \leq k$, for $k = 1, \ldots, n$ and $i \in [1, 2^n]$, we have $\mathsf{sk} \leftarrow K(\mathsf{pk}, m, \sigma^{(1)}, \ldots, \sigma^{(2n)})$ with non-negligible probability.

Given an n-generic signature scheme, we associate to it the problem $\mathbf{P}$ of computing sk from pk such that $\mathsf{Test}(\mathsf{pk}, \mathsf{sk}) = 1$. The following theorem states that all n-generic signature schemes satisfying n-soundness are existentially unforgeable under adaptively chosen-message attacks in the random-oracle model.

Theorem 3 (Security of n-Generic Signature Schemes) *Let* S *be an n-generic signature scheme satisfying n-soundness with underlying intractable hard problem $\mathbf{P}$. Let κ be the security parameter. Then,* S *is existentially unforgeable under adaptively chosen-message attacks in the random-oracle model.*

Proof We assume that the underlying problem $\mathbf{P}$ of the n-generic signature scheme is hard, i.e., for all PPT algorithms $\mathcal{A}$ the probability to solve a hard instance of $\mathbf{P}$ is negligible. Now, assume by contradiction, that S is *not* existentially unforgeable under chosen-message attacks. That is, there exists a PPT algorithm $\mathcal{B}_1$ such that $\mathcal{B}_1$ is able to output a signature $\sigma = (\sigma_0, h_1, \ldots, \sigma_{n-1}, h_n, \sigma_n)$ for a fresh message m^* with non-negligible probability. Then, due to the Extended Forking Lemma (Theorem 1) and the Nested Forking Lemma (Theorem 2) from Section 3.3, one can construct a PPT algorithm $\mathcal{B}_2$ which outputs 2^n correlated distinct valid signatures $\sigma^{(i)}$ for $i \in [1, 2^n]$, all on the same message m, as required in the statement of this theorem.

Due to the n-soundness of S, we know that there exists an "extractor" which, starting from these 2^n signatures on a message m, extracts the secret key. This contradicts the assumption that the underlying problem $\mathbf{P}$ is hard, and by implication, we conclude that there cannot exist such a successful forger $\mathcal{B}_1$. □

5.2 n-Generic Signature Schemes derived from Identification Schemes

Our goal is to enlarge the class of identification protocols to which the Fiat-Shamir transformation can be applied. We identify a potential set of candidates that we name *n-canonical identification schemes*. By n-canonical identification we mean schemes secure with respect to impersonation against passive attacks, where the challenges are drawn from an uniform distribution in exponential-sized sets and have $2n + 1$ moves.

Definition 5 (n-canonical Identification) An n-canonical identification scheme $\mathrm{IS} = (\mathcal{K}, \mathcal{P}, \mathcal{V})$ is a $(2n + 1)$-pass interactive protocol. $\mathcal{K}$ and $\mathcal{P} = (\mathsf{P}_1, \ldots, \mathsf{P}_{n+1})$

are PPT algorithms whereas $\mathcal{V} = (\mathsf{ChSet}, \mathsf{Vf})$ with ChSet being a PPT algorithm and Vf being a deterministic boolean algorithm. These algorithms are defined as follows:

$\mathcal{K}(1^\kappa)$ upon input a security parameter 1^κ, outputs a secret and public key pair $(\mathsf{sk}, \mathsf{pk})$ and challenge spaces $G_1, \ldots, G_n$ with $1/|G_i|$ negligible in 1^κ.
$\mathsf{P}_1(\mathsf{sk})$ upon input a secret key sk outputs the commitment R_1.
$\mathsf{P}_i(\mathsf{sk}, R_1, C_1, \ldots, R_{i-1}, C_{i-1})$ for $i = 2, \ldots, n$, upon input a secret key sk and the current transcript $R_1, C_1, \ldots, R_{i-1}, C_{i-1}$, outputs the i-th commitment R_i.
$\mathsf{P}_{n+1}(\mathsf{sk}, R_1, C_1, \ldots, R_n, C_n)$ upon input a secret key sk and the current transcript $R_1, C_1, \ldots, R_n, C_n$, outputs a response Rsp.
$\mathsf{ChSet}(\mathsf{pk}, i)$ upon input a public key pk and round number i, outputs a challenge $C_i \in G_i$.
$\mathsf{Vf}(\mathsf{pk}, R_1, C_1, \ldots, R_n, C_n, Rsp)$ upon input a public key pk, and the current transcript $R_1, C_1, \ldots, R_n, C_n, Rsp$, outputs either 1 (= valid) or 0 (= invalid).

We denote by $\langle \mathcal{P}(\mathsf{sk}, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle$ the transcript of an execution of an identification scheme. An n-canonical identification scheme IS has the following properties:

Public-Coin. For any index $i \in \{1, \ldots, n\}$ and any $(\mathsf{sk}, \mathsf{pk}, G_1, \ldots, G_n) \leftarrow \mathcal{K}(1^\kappa)$ the challenge $C_i \leftarrow \mathsf{ChSet}(\mathsf{pk}, i)$ is uniform in G_i.
Honest-Verifier Zero-Knowledge. There exists a PPT algorithm Z, the zero-knowledge simulator, such that for any pair of PPT algorithms $D = (D_0, D_1)$ the following distributions are computationally indistinguishable:
- Let $(\mathsf{pk}, \mathsf{sk}, st) \leftarrow D_0(1^\kappa)$. If $\mathsf{Test}(\mathsf{pk}, \mathsf{sk}) = 1$, set
$$trans = (R_1, C_1, \ldots, R_n, C_n, Rsp) \leftarrow \langle \mathcal{P}(\mathsf{sk}, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle ;$$
otherwise, set $trans \leftarrow \perp$. Output $D_1(trans, state)$.
- Let $(\mathsf{pk}, \mathsf{sk}, st) \leftarrow D_0(1^\kappa)$. If $\mathsf{Test}(\mathsf{pk}, \mathsf{sk}) = 1$, set
$$trans = (R_1, C_1, \ldots, R_n, C_n, Rsp) \leftarrow Z(\mathsf{pk}, 1) ;$$
otherwise set $trans \leftarrow Z(\mathsf{pk}, 0)$. Output $D_1(trans, state)$.

Note that the definition of 1-canonical identification schemes is identical to that of canonical identification schemes [1]. The Extended Fiat-Shamir transform that we have put forward can be applied to n-canonical identification schemes, thus yielding n-generic signature schemes. This is analogous to the original Fiat-Shamir transform when applied to a 1-canonical identification scheme [21]. The idea of this transformation consists on replacing the uniformly sampled challenges of the verifier output by ChSet by the outputs of hash functions $\mathrm{H}_i : \{0,1\}^* \to G_i$ modeled as random oracles. More precisely, let $\mathrm{IS} = (\mathcal{K}, \mathcal{P}, \mathcal{V})$ be an n-canonical identification scheme. The joint execution of $\mathcal{P}(\mathsf{sk}, \mathsf{pk})$ and $\mathcal{V}(\mathsf{pk})$ then defines an interactive protocol between the prover $\mathcal{P}$ and the verifier $\mathcal{V}$. At the end of the protocol $\mathcal{V}$ outputs a decision bit $b \in \{0, 1\}$. An n-generic signature scheme $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ is derived as follows:

$\mathsf{KGen}(1^\kappa)$ takes as input a security parameter 1^κ and returns $\mathcal{K}(1^\kappa)$.
$\mathsf{Sign}(\mathsf{sk}, m)$ takes as input a secret key sk and a message m and returns the transcript $\langle \mathcal{P}(\mathsf{sk}, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle$ as the signature σ, i.e., $\sigma = (\sigma_0, h_1, \ldots, h_n, \sigma_n) = (R_1, C_1, \ldots, R_n, C_n, Rsp)$, where $C_i := \mathrm{H}_i(m, R_1, C_1, \ldots, R_{i-1}, C_{i-1}, R_i)$.

$\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ takes as input a public key pk, a message m and a signature σ and returns $\mathcal{V}.\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ as the decision bit.[4]

The resulting scheme S is an n-generic signature scheme if $R_1, C_1, \ldots, R_{n-1}$ has a min-entropy of $\omega(|H_n|)$. Indeed, the obtained scheme S has the right structure and the honest-verifier zero-knowledge property is guaranteed by (the similar property of) the identification scheme.

However, it is still not guaranteed that S is existentially unforgeable. It lacks then to check/prove that the resulting scheme S is n-sound. If this is the case then one can apply Theorem 3 to obtain existential unforgeability against adaptive chosen-message attacks.

Let us point out that the plain version of most identification protocols does not directly satisfy the required security level by their choice of challenges spaces $G_1, \ldots, G_n$. In particular, it might be the case that $1/|G_i|$ is not negligible in the security parameter 1^κ. For that reason, one should typically repeat the ID protocol several (say δ) times until the desired security level is reached. In that case the concatenation of δ transcripts $\langle \mathcal{P}(\mathsf{sk}, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle$ builds the signature (instead of a single execution of the ID scheme). Note here that the challenges for all protocol executions are computed by a single call to the hash function on input all commitments. This is mandatory since, otherwise, the probability to forge grows linearly with δ instead of exponentially. Moreover, for our security analysis, we consider that the commitments R_i contain more entropy than k_n, the output size of the last hash function. This condition can be achieved by choosing their domain as large as necessary. Note that in [21] it is assumed that R_1 is uniformly distributed over its corresponding set.

Many zero-knowledge identification schemes have been proposed, whose conversion to signature schemes does not lead to generic signature schemes according to the definition of Pointcheval and Stern [21]. Examples of such schemes are those based on the Permuted Kernel Problem [24,17], the Permuted Perceptron Problem [19,20], the Constrained Linear Equations [27], the five-pass variant of SD problem [26,2], the q-SD problem [8], the SIS problem [7,25] and the MQ-problem [23]. Fortunately, their conversion to signature schemes belong to the class of n-generic signature schemes. Unlike [19,20], they even satisfy 2-soundness. Consequently, our result for the security of n-generic signature schemes satisfying n-soundness carries over to the resulting signature schemes derived from all these aforementioned identification schemes in the random-oracle model.

Next, we provide the security argument for two resulting signature schemes. The first one is obtained from the q-SD code-based identification scheme [8] and the second one is derived from the MQ-based identification scheme [23]. For the remaining aforementioned identification schemes the argument is formulated in a very similar fashion. For this reason, we omit those proofs here.

5.3 The 5-pass q-SD Code-based Identification Scheme [8] and its Signature

At CRYPTO 1993, Stern proposed an efficient code-based identification scheme using binary random codes, which is still today the reference in this area [26]. In

[4] By $\mathcal{V}.\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ we mean the verification algorithm performed by the verifier from the underlying identification scheme IS.

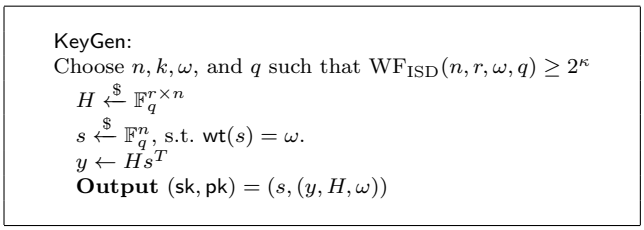

Fig. 2 CVE key generation algorithm.

2010, Cayrel, Véron, and El Yousfi presented in [8] a five-pass identification (q-SD) scheme using q-ary codes instead of binary codes. The main achievement of this proposal is to decrease the cheating probability of each round from 2/3 for Stern's scheme to 1/2 for their new scheme. This allows to decrease the communication complexity by obtaining the same impersonation probability in fewer rounds compared to Stern construction. Furthermore, the q-SD scheme is proven to satisfy the zero-knowledge property and its security is based on the hardness of the q-ary Syndrome Decoding problem.

In what follows, the elements of $\mathbb{F}_q^n$ are written as n blocks of size $\lceil \log_2(q) \rceil = N$ and each element of $\mathbb{F}_q$ as N bits. We denote by $\mathsf{wt}(v)$ the hamming weight of vector v.

Before presenting the q-SD identification scheme, we first introduce a special transformation that is used in the protocol.

Definition 6 *Let Σ be a permutation of $\{1, \ldots, n\}$ and $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{F}_q^n$ such that $\forall i, \gamma_i \neq 0$. We define the transformation $\Pi_{\gamma,\Sigma}$ as :*

$$\begin{aligned} \Pi_{\gamma,\Sigma} : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^n \\ v &\mapsto (\gamma_{\Sigma(1)} v_{\Sigma(1)}, \ldots, \gamma_{\Sigma(n)} v_{\Sigma(n)}) \end{aligned}$$

Notice that $\forall \alpha \in \mathbb{F}_q$, $\forall v \in \mathbb{F}_q^n$, $\Pi_{\gamma,\Sigma}(\alpha v) = \alpha \Pi_{\gamma,\Sigma}(v)$, and $\mathsf{wt}(\Pi_{\gamma,\Sigma}(v)) = \mathsf{wt}(v)$.

The q-SD scheme consists of two parts: a key generation algorithm and an ID protocol described in Figure 2 and 3, respectively. In the following we describe these two parts.

The q-SD Key Generation Algorithm. Let κ be the security parameter and $n, r = n - k, \omega$ be chosen accordingly. The q-SD scheme uses a random $(r \times n)$ q-ary matrix H common to all users which can be considered to be the parity check matrix of a random linear $[n, k, \omega]$ q-ary code. We can assume that H is described as $(I_r|R)$ where R is a random $r \times r$ matrix; as Gaussian elimination does not change the code generated by H, there is no loss of generality. Figure 2 presents the key generation algorithm.

The q-SD Protocol. The secret key holder can prove his knowledge of s by using two blending factors: a random vector and a special transformation which has the advantage to hide the non-zero values of the secret s. The security of the q-SD scheme relies on the hardness of the syndrome decoding problem defined over $\mathbb{F}_q$, i.e., on the difficulty of determining the preimage s of $y = Hs^T$.

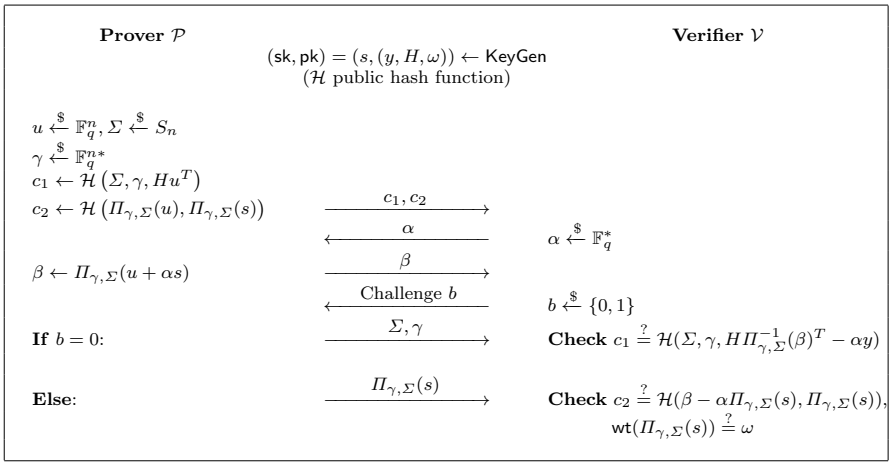

Fig. 3 The CVE identification protocol

The resulting Signature Scheme. According to Section 5.2, the q-SD identification scheme described above can be turned to an n-generic signature scheme $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ as follows. Let δ be the number of rounds needed to achieve the required impersonation resistance.

$\mathsf{KGen}(1^\kappa)$ takes as input a security parameter 1^κ and outputs $\mathcal{K}(1^\kappa)$. The random oracles $\mathcal{O}_1$ and $\mathcal{O}_2$ output elements of $\mathbb{F}_q^\delta$ and $\{0,1\}^\delta$, respectively.

$\mathsf{Sign}(\mathsf{sk}, m)$ takes as input sk (as defined in Figure 2) and a message m, and computes for all $1 \le i \le \delta$,

- $c_{0,i} = \mathcal{H}\left(\Sigma_i, \gamma_i, Hu_i^T\right), c_{1,i} = \mathcal{H}\left(\Pi_{\gamma_i,\Sigma_i}(u_i), \Pi_{\gamma_i,\Sigma_i}(s)\right)$, and sets $\sigma_{0,i} = (c_{0,i}, c_{1,i})$, where $u_i \xleftarrow{\$} \mathbb{F}_q^n, \Sigma_i \xleftarrow{\$} S_n$, and $\gamma_i \xleftarrow{\$} \mathbb{F}_q^{n*}$
- $h_1 = \mathcal{O}_1(m, \sigma_{0,1}, \ldots, \sigma_{0,\delta})$ with $h_1 = (h_{1,1}, \ldots h_{1,\delta}) \in \mathbb{F}_q^\delta$,
- $\sigma_{1,i} = \Pi_{\gamma_i,\Sigma_i}(u_i + h_{1,i}s)$,
- sets $h_2 = \mathcal{O}_2(m, \sigma_0, h_1, \sigma_1)$, where $\sigma_j = (\sigma_{j,1}, \ldots, \sigma_{j,\delta})$ with $0 \le j \le 1$, $h_2 = (h_{2,1}, \ldots, h_{2,\delta}) \in \{0,1\}^\delta$,
- and finally, returns the signature σ for the message m as $(\sigma_0, h_1, \sigma_1, h_2, \sigma_2)$, where $\sigma_2 = (\sigma_{2,1}, \ldots, \sigma_{2,\delta})$ such that $\sigma_{2,i} = (\gamma_i, \Sigma_i)$ if $h_{2,i} = 0$ and, otherwise, $\sigma_{2,i} := \Pi_{\gamma_i,\Sigma_i}(s)$.

$\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ takes as input a public key pk (as defined in Figure 2), a message m and a signature σ, and outputs 1 iff $(\sigma_{0,1}, \ldots, \sigma_{0,\delta})$ is well calculated as in the ID protocol, i.e., the following respective equation is valid for all $1 \le i \le \delta$:

$$\begin{aligned} &\text{If } h_{2,i} = 0: \; c_{0,i} = \mathcal{H}(\Sigma_i, \gamma_i, H\Pi^{-1}_{\gamma_i,\Sigma_i}(\sigma_{1,i})^T - h_{1,i}y) \\ &\text{If } h_{2,i} = 1: \; c_{1,i} = \mathcal{H}(\sigma_{1,i} - h_{1,i}\Pi_{\gamma_i,\Sigma_i}(s), \Pi_{\gamma_i,\Sigma_i}(s)) \\ &\qquad\qquad \wedge \quad \mathsf{wt}(\Pi_{\gamma_i,\Sigma_i}(s)) \stackrel{?}{=} \omega \; . \end{aligned}$$

Security Argument. To obtain this security reduction we will apply the Nested Forking Lemma (Theorem 1) with $n = 2$. Firstly we see that the qSD signature scheme is a 2-generic signature scheme. This is implied by the fact that it has been obtained through the 5-pass Fiat-Shamir transform and that the original

5-pass IS scheme is proven to be honest-verifier zero-knowledge in [8]. Let us choose an integer j such that $1 \leq j \leq \delta$, and let us point out that every atomic signature $(\sigma_{0,j}, h_{1,j}, \sigma_{1,j}, h_{2,j}, \sigma_{2,j})$ can be also seen as a 2-signature scheme. Thus, from a successful forger against the 2-generic qSD signature scheme, and for any $1 \leq j \leq \delta$, we obtain with non-negligible probability 4 distinct forgeries for the same message m

- $(\sigma_{0,j}, \sigma_{1,j}^{(1)}, \sigma_{2,j}^{(1)}, h_{1,j}^{(1)}, h_{2,j}^{(1)})$,
- $(\sigma_{0,j}, \sigma_{1,j}^{(2)}, \sigma_{2,j}^{(2)}, h_{1,j}^{(2)}, h_{2,j}^{(2)})$,
- $(\sigma_{0,j}, \sigma_{1,j}^{(3)}, \sigma_{2,j}^{(3)}, h_{1,j}^{(3)}, h_{2,j}^{(3)})$,
- $(\sigma_{0,j}, \sigma_{1,j}^{(4)}, \sigma_{2,j}^{(4)}, h_{1,j}^{(4)}, h_{2,j}^{(4)})$,

where $h_{1,j}^{(1)} \neq h_{1,j}^{(2)}$, $(h_{1,j}^{(1)}, \sigma_{1,j}^{(1)}) = (h_{1,j}^{(3)}, \sigma_{1,j}^{(3)})$, $(h_{1,j}^{(2)}, \sigma_{1,j}^{(2)}) = (h_{1,j}^{(4)}, \sigma_{1,j}^{(4)})$, $h_{2,j}^{(2)} \neq h_{2,j}^{(3)}$ and $h_{2,j}^{(1)} \neq h_{4,j}^{(2)}$.

For each index j with $1 \leq j \leq \delta$, we have then

1. $h_{1,i}^{(1)} \neq h_{1,i}^{(2)}$ (say $h_{1,i}^{(1)} = \alpha \in \mathbb{F}_q$ and and $h_{1,i}^{(2)} = \alpha' \in \mathbb{F}_q$)
2. $h_{2,j}^{(2)} \neq h_{2,j}^{(3)}$ (say $h_{2,j}^{(2)} = 0$ and $h_{2,j}^{(3)} = 1$)
3. $h_{2,j}^{(1)} \neq h_{4,j}^{(2)}$ (say $h_{2,j}^{(1)} = 0$ and $h_{4,j}^{(2)} = 1$)

Let (μ, τ), $\bar{z}$, (μ', τ'), $\tilde{z}$ the values parsed from $\sigma_{2,i}^{(1)}, \sigma_{2,i}^{(2)}, \sigma_{2,i}^{(3)}, \sigma_{2,i}^{(4)}$, and let us rename $\sigma_{1,j} := \sigma_{1,j}^{(1)} = \sigma_{1,j}^{(3)}$ and $\sigma'_{1,j} := \sigma_{1,j}^{(2)} = \sigma_{1,j}^{(4)}$. Then, since $\sigma_{0,i}$ is fixed for the 4 atomic signatures :

$$c_{0,i} = \mathcal{H}(m, \mu, \tau, {H\Pi_{\mu,\tau}}^{-1}(\sigma_{1,i}) - \alpha y) = \mathcal{H}(m, \mu', \tau', {H\Pi_{\mu',\tau'}}^{-1}({\sigma'}_{1,i}) - \alpha' y)$$

$$c_{1,i} = \mathcal{H}(\sigma_{1,i} - \alpha\bar{z}, \bar{z}) = \mathcal{H}({\sigma'}_{1,i} - \alpha'\tilde{z}, \tilde{z}) \text{ and } \omega(\bar{z}) = \omega(\tilde{z}) = \omega$$

Hence either we have found a collision for the hash function or

$$\mu = \mu', \tau = \tau', \bar{z} = \tilde{z}, \sigma_{1,i} - {\sigma'}_{1,i} = (\alpha - \alpha')\bar{z}$$

$${H\Pi_{\mu,\tau}}^{-1}(\sigma_{1,i} - {\sigma'}_{1,i}) = (\alpha - \alpha')y$$

frow which we deduce that

$$H\bar{z} = y \text{ and } \omega(\bar{z}) = p$$

which is a solution to the SD problem. This proves the existence of an extractor as specified in 2-soundness. The latter property, together with 2-generic signature property, imply by virtue of Theorem 3, that our q-SD signature scheme is existentially unforgeable under the hardness of the syndrome decoding problem in the random oracle model. □

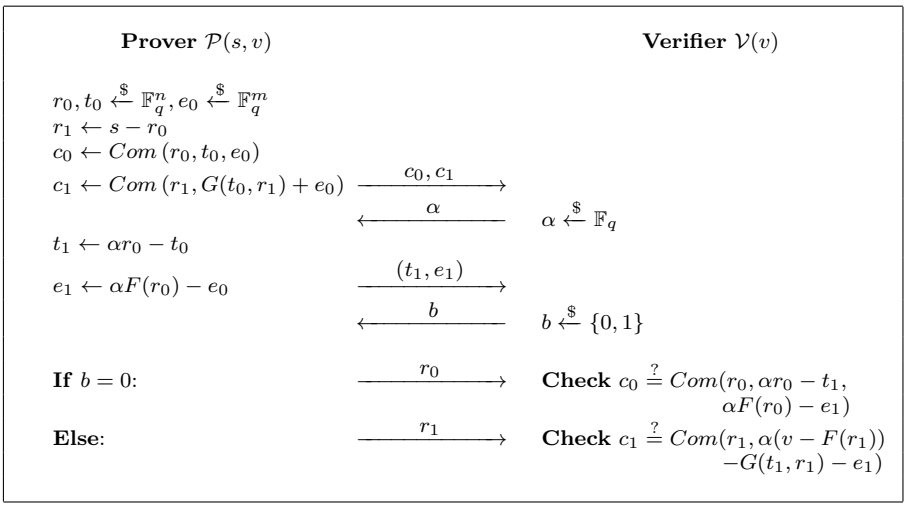

Fig. 4 The five-pass MQ identification scheme

5.4 The 5-pass MQ Identification Scheme [23] and its Signature

Recently at CRYPTO 2011, Sakumoto et al. presented a five-pass identification scheme based on multivariate quadratic polynomials [23]. Assuming the existence of a non-interactive commitment scheme Com which should be statistically hiding and computationally binding, the authors of [23] showed that their scheme is an honest-verifier zero-knowledge identification scheme. Actually, 2-soundness is also satisfied, as we will see below.

First, we briefly describe the identification scheme [23]; then, we detail the procedure to convert it into a signature scheme using Section 5.2; finally, we analyze the security of the obtained signature scheme using the Extended Forking Lemma from Section 3.3.

Let n, m and q be positive integers. We denote by $\mathcal{MQ}(n, m, \mathbb{F}_q)$ a family of functions

$$\left\{ F(x) = (f_1(x), \cdots, f_m(x)) \ : \ \begin{array}{l} f_l(x) = \sum_{i,j} a_{l,i,j} x_i x_j + \sum_i b_{l,i} x_i, \\ a_{l,i,j}, b_{l,i} \in \mathbb{F}_q \text{ for } l = 1, \ldots, m \end{array} \right\}$$

where $x = (x_1, \cdots, x_n)$. An element F of $\mathcal{MQ}(n, m, \mathbb{F}_q)$ is called an MQ function and a function $G(x, y) = F(x + y) - F(x) - F(y)$ is called the polar form of F.

Let κ be a security parameter. Let $n = n(\kappa), m = m(\kappa)$ and $q = q(\kappa)$ be polynomially bounded functions. The key-generation algorithm $\mathcal{K}$ of this identification scheme can be described as follows. It takes 1^κ as input and creates a system parameter $F \in \mathcal{MQ}(n, m, \mathbb{F}_q)$ which consists of an m-tuple of random multivariate quadratic polynomials. Then, it randomly chooses a vector $s \in \mathbb{F}_q^n$ (secret key), and computes the corresponding public key $v := F(s)$. Finally, it outputs the key pair $(\mathsf{pk}, \mathsf{sk}) = (v, s)$. Figure 4 illustrates the interaction protocol between the prover and the verifier.

The resulting Signature Scheme. We will use the results from Section 5.2 to turn the MQ-based identification scheme described above can into a 2-generic signature scheme $\mathrm{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vf})$ as follows. Let δ be the number of rounds needed to achieve the required impersonation resistance.

$\mathsf{KGen}(1^\kappa)$ takes as input a security parameter 1^κ and outputs $\mathcal{K}(1^\kappa)$. The random oracles $\mathcal{O}_1$ and $\mathcal{O}_2$ output elements of $\mathbb{F}_q^\delta$ and $\{0,1\}^\delta$, respectively, and are obtained by a parallel computation of random oracles $\mathcal{O}_{1,i}, \mathcal{O}_{2,i}$ for $1 \le i \le \delta$.

$\mathsf{Sign}(\mathsf{sk}, m)$ takes as input sk and a message m, and computes for all $1 \le i \le \delta$,

- $r_{1,i} = s - r_{0,i}$ where $r_{0,i} \xleftarrow{\$} \mathbb{F}_q^n$,
- $c_{0,i} = Com\left(r_{0,i}, t_{0,i}, e_{0,i}\right), c_{1,i} = Com\left(r_{1,i}, G(t_{0,i}, r_{1,i}) + e_{0,i}\right)$, and sets $\sigma_{0,i} = (c_{0,i}, c_{1,i})$, where $t_{0,i} \xleftarrow{\$} \mathbb{F}_q^n$ and $e_{0,i} \xleftarrow{\$} \mathbb{F}_q^m$,
- $h_1 = \mathcal{O}_1(m, \sigma_{0,1}, \ldots, \sigma_{0,\delta}) = (h_{1,1}, \ldots h_{1,\delta}) \in \mathbb{F}_q^\delta$ where $h_{1,i} := \mathcal{O}_{1,i}(m, \sigma_{0,1}, \ldots, \sigma_{0,\delta})$, for $1 \le i \le \delta$,
- $(t_{1,i}, e_{1,i}) = (h_{1,i} \cdot r_{0,i} - t_{0,i}, h_{1,i} \cdot F(r_{0,i}) - e_{0,i})$ and sets $\sigma_{1,i} = (t_{1,i}, e_{1,i})$,
- sets $h_2 = (h_{2,1}, \ldots, h_{2,\delta}) = \mathcal{O}_2(m, \sigma_0, h_1, \sigma_1)$, where $\sigma_j = (\sigma_{j,1}, \ldots, \sigma_{j,\delta})$ and $h_{2,i} := \mathcal{O}_{2,i}(m, \sigma_0, h_1, \sigma_1)$ for $0 \le j \le 1$ and $1 \le i \le \delta$,
- and finally, returns the signature σ for the message m as $(\sigma_0, h_1, \sigma_1, h_2, \sigma_2)$, where $\sigma_2 = (\sigma_{2,1}, \ldots, \sigma_{2,\delta})$ such that $\sigma_{2,i} := r_{0,i}$ if $h_{2,i} = 0$ and, otherwise, $\sigma_{2,i} := r_{1,i}$.

$\mathsf{Vf}(\mathsf{pk}, m, \sigma)$ takes as input a public key pk, a message m and a signature $\sigma = (\sigma_0, h_1, \sigma_1, h_2, \sigma_2)$. It parses

$$\sigma_0 = \big(\ (c_{0,1}, c_{1,1}), \ldots, (c_{0,\delta}, c_{1,\delta})\ \big),$$
$$h_1 = (h_{1,1}, \ldots h_{1,\delta}) \in \mathbb{F}_q^\delta,$$
$$\sigma_1 = \big(\ (t_{1,1}, e_{1,1}), \ldots, (t_{1,\delta}, e_{1,\delta})\ \big) \in \left(\mathbb{F}_q^n \times \mathbb{F}_q^m\right)^\delta,$$
$$h_2 = (h_{2,1}, \ldots, h_{2,\delta}) \in \{0,1\}^\delta,$$
$$\sigma_2 = (\sigma_{2,1}, \ldots, \sigma_{2,\delta}),$$

and outputs 1 iff the following equation is valid for all $1 \le i \le \delta$:

$$\text{If } h_{2,i} = 0: \ c_{0,i} = Com\left(\sigma_{2,i}, h_{1,i} \cdot \sigma_{2,i} - t_{1,i}, h_{1,i} \cdot F(\sigma_{2,i}) - e_{1,i}\right).$$
$$\text{If } h_{2,i} = 1: \ c_{1,i} = Com\left(\sigma_{2,i}, h_{1,i}(v - F(\sigma_{2,i})) - G(t_{1,i}, \sigma_{2,i}) - e_{1,i}\right).$$

Security Argument[5]. To obtain this security reduction we will apply the Nested Forking Lemma (Theorem 1) with $n = 2$. Firstly we see that the MQ signature scheme is a 2-generic signature scheme. This is implied by the fact that it has been obtained through the 5-pass Fiat-Shamir transform and that the original 5-pass IS scheme is proven to be honest-verifier zero-knowledge in [23]. Let us choose an integer j such that $1 \le j \le \delta$, and let us point out that every atomic signature $(\sigma_{0,j}, h_{1,j}, \sigma_{1,j}, h_{2,j}, \sigma_{2,j})$ can be also seen a 2-signature scheme. Thus, from a successful forger against the 2-generic MQ signature scheme, and for any $1 \le j \le \delta$, we obtain with non-negligible probability 4 distinct forgeries for the same message m

- $(\sigma_{0,j}, \sigma_{1,j}^{(1)}, \sigma_{2,j}^{(1)}, h_{1,j}^{(1)}, h_{2,j}^{(1)})$,
- $(\sigma_{0,j}, \sigma_{1,j}^{(2)}, \sigma_{2,j}^{(2)}, h_{1,j}^{(2)}, h_{2,j}^{(2)})$,

[5] In the conference version of this work [3] a simpler security argument was given that turned out be flawed.

– $(\sigma_{0,j}, \sigma_{1,j}^{(3)}, \sigma_{2,j}^{(3)}, h_{1,j}^{(3)}, h_{2,j}^{(3)})$,
– $(\sigma_{0,j}, \sigma_{1,j}^{(4)}, \sigma_{2,j}^{(4)}, h_{1,j}^{(4)}, h_{2,j}^{(4)})$,

where $h_{1,j}^{(1)} \neq h_{1,j}^{(2)}$, $(h_{1,j}^{(1)}, \sigma_{1,j}^{(1)}) = (h_{1,j}^{(3)}, \sigma_{1,j}^{(3)})$, $(h_{1,j}^{(2)}, \sigma_{1,j}^{(2)}) = (h_{1,j}^{(4)}, \sigma_{1,j}^{(4)})$, $h_{2,j}^{(2)} \neq h_{2,j}^{(3)}$ and $h_{2,j}^{(1)} \neq h_4^{(2)}$. Thus we obtain for each j-th atomic signature four forgeries satisfying the conditions stated in Theorem 5 in [23], for $1 \leq j \leq \delta$. This implies that any attacker against our signature scheme can be turned with non-negligible probability into a solver of the MQ problem or into an attacker against the binding property of the commitment scheme in the random oracle model. □

Acknowledgements We are thankful to an anonymous reviewer for pointing out that our security reduction for the MQ signature scheme in the conference version of this manuscript was incomplete. This observation lead us to a new reshaping of our previous work. This work has received funding from the German Federal Ministry of Education and Research (BMBF) within EC SPRIDE, the Hessian LOEWE excellence initiative within CASED and the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 258865.

References

1. Abdalla, M., An, J.H., Bellare, M., Namprempre, C.: From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In: EUROCRYPT'02, pp. 418–433. Springer (2002)
2. Aguilar Melchor, C., Gaborit, P., Schrek, J.: A new zero-knowledge code based identification scheme with reduced communication. CoRR **abs/1111.1644** (2011)
3. Alaoui, S.M.E.Y., Dagdelen, Ö., Véron, P., Galindo, D., Cayrel, P.L.: Extended security arguments for signature schemes. In: A. Mitrokotsa, S. Vaudenay (eds.) AFRICACRYPT, *Lecture Notes in Computer Science*, vol. 7374, pp. 19–34. Springer (2012)
4. Bellare, M., Neven, G.: Multi-signatures in the plain public-key model and a general forking lemma. In: Proceedings of the 13th ACM conference on Computer and communications security, CCS '06, pp. 390–399. ACM, New York, NY, USA (2006)
5. Bitansky, N., Dachman-Soled, D., Garg, S., Jain, A., Kalai, Y., Lpez-Alt, A., Wichs, D.: Why fiat-shamir for proofs lacks a proof. In: A. Sahai (ed.) Theory of Cryptography, *Lecture Notes in Computer Science*, vol. 7785, pp. 182–201. Springer Berlin Heidelberg (2013)
6. Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: ASIACRYPT, pp. 41–69 (2011)
7. Cayrel, P.L., Lindner, R., Rückert, M., Silva, R.: Improved zero-knowledge identification with lattices. In: ProvSec'10, pp. 1–17. Springer (2010)
8. Cayrel, P.L., Véron, P., El Yousfi Alaoui, S.M.: A zero-knowledge identification scheme based on the q-ary syndrome decoding problem. In: SAC'2010, LNCS, pp. 170–186. Springer (2010)
9. Cramer, R.: Modular design of secure, yet practical cryptographic protocols. Ph.D. thesis, University of Amsterdam (1996)
10. Dagdelen, Ö., Fischlin, M., Gagliardoni, T.: The fiat-shamir transformation in a quantum world. In: ASIACRYPT (2), pp. 62–81 (2013)
11. Dagdelen, Ö., Venturi, D.: A second look at fischlin's transformation. In: AFRICACRYPT, pp. 356–376 (2014)
12. Fiat, A., Shamir, F.: How to prove yourself: practical solutions to identification and signature problems. In: CRYPTO'86, pp. 186–194. Springer (1987)
13. Fischlin, M.: Communication-efficient non-interactive proofs of knowledge with online extractors. In: CRYPTO, pp. 152–168 (2005)
14. Gamal, T.E.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: CRYPTO'84, pp. 10–18. Springer (1985)

15. Goldwasser, S., Kalai, Y.: On the (in)security of the fiat-shamir paradigm. In: 44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings., pp. 102–113 (2003)
16. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems. In: STOC '85, pp. 291–304. ACM (1985)
17. Lampe, R., Patarin, J.: Analysis of Some Natural Variants of the PKP Algorithm. In: J.Z.E. Pierangela Samarati Wenjing Lou (ed.) SECRYPT 2012 - Proceedings of the International Conference on Security and Cryptography, pp. 209–2014. SciTePress (2012)
18. Ohta, K., Okamoto, T.: On concrete security treatment of signatures derived from identification. In: CRYPTO'98, pp. 354–369 (1998)
19. Pointcheval, D.: A new identification scheme based on the perceptrons problem. In: EUROCRYPT'95, pp. 319–328. Springer (1995)
20. Pointcheval, D., Poupard, G.: A new NP-complete problem and public-key identification. Des. Codes Cryptography **28**, 5–31 (2003)
21. Pointcheval, D., Stern, J.: Security proofs for signature schemes. In: EUROCRYPT'96, pp. 387–398. Springer (1996)
22. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptology **13**(3), 361–396 (2000)
23. Sakumoto, K., Shirai, T., Hiwatari, H.: Public-key identification schemes based on multivariate quadratic polynomials. In: CRYPTO'11, *LNCS*, vol. 6841, pp. 706–723. Springer (2011)
24. Shamir, A.: An efficient identification scheme based on permuted kernels (extended abstract). In: CRYPTO'89, pp. 606–609. Springer (1990)
25. Silva, R., Cayrel, P.L., Lindner, R.: Zero-knowledge identification based on lattices with low communication costs. XI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais **8**, 95–107 (2011)
26. Stern, J.: A new identification scheme based on syndrome decoding. In: CRYPTO'93, pp. 13–21. Springer (1993)
27. Stern, J.: Designing identification schemes with keys of short size. In: CRYPTO'94, pp. 164–173. Springer (1994)
28. Yao, A.C.C., Zhao, Y.: Online/offline signatures for low-power devices. IEEE Transactions on Information Forensics and Security **8**(2), 283–294 (2013)